REMARKS

Claims 1-36 are pending in the application.

Claims 1-24 and 26-36 are rejected.

Claims 1-24 and 26-36 remain pending in the application.

Applicants respectfully request reconsideration in light of the remarks contained herein.

Claim Rejections - 35 U.S.C. § 103

Claims 1-3, 6-8, 10-12, 14-20, 22-24, 26-30, and 32-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over "Secure communications Over Insecure Channels," by Ralph C. Merkle, hereinafter *Merkle*, in view of U.S. Patent No. 5,481,613 to Ford et al., hereinafter *Ford*.

Applicant respectfully submits that *Merkle* and *Ford*, alone or in combination, do not disclose each element of Claim 1. For example, the Applicant respectfully submits that neither *Merkle* nor *Ford* disclose "adding randomization information at the receiver to the corresponding token of the selected trap door encryption-decryption function pair; [and] encrypting the token with the added randomization information at the receiver, the token corresponding with the randomly selected encryption-decryption function pair," as required by Claim 1.

The Examiner states that:

> Merkle does not disclose adding randomization information at the receiver to the corresponding token of the selected trap door encryption-decryption function pair and encrypting the token with the added randomization information, the token corresponding with the randomly selected encryption-decryption function pair.
>
> Ford teaches returning the identifier back to the key release agent in a locally protected transaction (column 4, lines 24-29; column 4, lines 50-54).
>
> It would have been obvious to one of ordinary skill in the ad **[sic]** at the time the invention was made to add randomization information at the receiver to the corresponding token of the selected trap door encryption-decryption function pair and encrypt the token with the added randomization information, the token corresponding with the randomly selected encryption-decryption function pair, as apposed to sending it back unencrypted as Merkle suggests, since Ford discloses at column 3, line 62 to column 4, line 12 that such a modification would allow secure distribution of an encryption key to client who are authorized according to a set of access control attributes, provide a method of recovering an encryption key from a key release agent in a secure manner, provide a method of recovering an encryption key from an encrypted access controlled decryption block which contain access control attributes, and provide a key release agent releasing an encryption key to a party other than a client that is explicitly authorized.

(Final Office Action, Page 4).

First, Applicant respectfully disagrees that *Ford*'s discussion of "returning the identifier back to the key release agent in a locally protected transaction," supplies the above-identified missing elements. The cited portions of *Ford* state that "[t]he method further includes steps of the decryptor sending to the key release agent the identifier and the access controlled decryption block in the locally protected transaction, the identifier indicating a key release private key corresponding to the key-release public key," (*Ford*, col. 4, lines 24-29) and "[t]he decryptor has transaction device for sending the access controlled decryption block and the identifier together with a set of decryptor attributes to the key release agent in a locally-protected transaction." (*Ford,* col. 4, lines 50-53) Neither of these passages discuss "**adding randomization information** at the receiver to the corresponding token of the selected trap door encryption-decryption function pair," as required by Claim 1. Similarly, neither of the cited passages discuss "encrypting the token **with the added randomization information** at the receiver, the token corresponding with the randomly selected encryption-decryption function pair," as required by Claim 1.

Furthermore, the Examiner's rationale for the combination of *Merkle* and *Ford* similarly fails to compensate for the deficiencies in *Merkle* and *Ford*. The Examiner cited *Ford*, col. 3, line 62-col. 4, line 12 to support his contention that it would have been obvious to add the missing claim elements. *Ford*, col. 3, line 62-col. 4, line 12, is a listing of the "Objects of The Invention" section of *Ford*, which does not mention "**adding randomization information** at the receiver to the corresponding token of the selected trap door encryption-decryption function pair," and "encrypting the token **with the added randomization information** at the receiver, the token corresponding with the randomly selected encryption-decryption function pair," as required by Claim 1.

Second, even assuming for purposes of argument that the proposed combination discloses the limitations of Applicant's claims, which Applicant disputes, it would not have been obvious to one skilled in the art to make the combination. The mere fact that references can be combined does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. *In re Mills,* 916 F.2d 680 (Fed. Cir. 1990). The showing must be clear and particular. *See, e.g., C.R. Bard v. M3 Sys., Inc.*, 48 USPQ.2d 1225, 1232 (Fed. Cir. 1998). The Examiner has not provided adequate evidence of the required motivation or suggestion to make the proposed combination. The Examiner merely cites "Objects of The Invention" section of *Ford* to support his contention that the combination of *Merkle* and *Ford* is

obvious to a person of ordinary skill in the art (Office Action, page 4). As the Applicant has demonstrated above, however, the "Objects of The Invention" section of *Ford* does not even disclose the missing claim elements, much less suggest their combination with another reference. The Examiner has not shown any motivation to combine and instead simply relies upon hindsight. It is improper for an Examiner to use hindsight having read the Applicant's disclosure to arrive at an obviousness rejection. *In re* Fine, 837 F.2d 1071, 1075, 5 U.S.P.Q.2d 1596, 1600 (Fed. Cir. 1988). It is improper to use the claimed invention as an instruction manual or template to piece together the teachings of the prior art so that the claimed invention is rendered obvious. *In re* Fritch, 972 F.2d 1260, 23 U.S.P.Q.2d 1780 (Fed. Cir. 1992). Because the Examiner has merely used Applicant's claims as an instruction manual to piece together the encryption system of *Merkle* with key distribution technique discussed in *Ford*, Applicant respectfully submits that the proposed *Merkle-Ford* combination is improper and should not be used here to reject Applicant's claims.

For at least these reasons, Applicant respectfully requests reconsideration and allowance of Claim 1.

The Examiner also relies on the *Merkle-Ford* combination to reject independent Claims 6, 14, 28, and 33. Applicant respectfully submits that the proposed *Merkle-Ford* combination does not disclose, teach, or suggest each and every element of Applicant's independent claims. Thus, for reasons similar to those discussed above with regard to Claim 1, Applicant respectfully submits that neither *Merkle* nor *Ford* disclose, teach, or suggest each and every element as set forth in Applicant's independent Claims 6, 14, 28, and 33.

Dependent Claims 2 and 3 depend from independent Claim 1, dependent Claims 7, 8, and 10-12 depend from independent Claim 6, dependent Claims 29-30 and 32 depend from independent Claim 28, and dependent claims 34-36 depend from independent Claim 33. Applicant has shown each of the independent claims to be allowable. Accordingly, dependent Claims 2, 3, 7, 8, 10-12, 29-30, 32, and 34-36 are not obvious over the *Merkle-Ford* combination at least because they include the limitations of their respective independent claims. Additionally, dependent Claims 2, 3, 7, 8, 10-12, 29-30, 32, and 34-36 recite elements that further distinguish the art. As just one example, Claim 3 recites "randomly selecting at the receiver an additional trap door encryption-decryption function pair and the corresponding token" and "adding randomization information to the corresponding token of the additional selected trap door

encryption-decryption function pair." Claims 7, 20, 22, 30, 34, and 36 recite certain similar, though not identical, features and operations. The Examiner acknowledges that *Merkle* does not explicitly teach the receiver selecting more than one of the puzzles to decrypt. (Final Office Action, page 4). The Examiner posits, however, that "one of ordinary skill in the art would know that the work needed to be performed by an eavesdropper plotting to learn the decryption key is O (n^2)" and that "[h]aving the receiver choose more than one puzzles **[sic]** slightly increases the poor security of Merkle's system by forcing the eavesdropper to perform more calculations." (Final Office Action, pages 4-5). The Examiner, however, has not cited any portion of *Merkle, Ford*, or any other reference to support his conclusion. Therefore, the Examiner's rejection of claims 3, 7, 20, 22, 30, 34, and 36 is improper. For reasons similar to those discussed above with regard to Claim 1, Applicant respectfully submits that neither *Merkle* nor *Ford* disclose, teach, or suggest the features and operations recited in dependent Claims 2, 3, 7, 8, 10-12, 29-30, 32, and 34-36. For at least these reasons, Applicant respectfully requests reconsideration and allowance of Claims 2, 3, 7, 8, 10-12, 29-30, 32, and 34-36.

Claims 4, 5, 9, 13, 21, and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Merkle*, in view of *Ford.*, and further in view of U.S. Patent No. 5,815,573 to Johnson, *et al.,* hereinafter *Johnson*. Dependent claims 4 and 5 depend from independent Claim 1, dependent claims 9, 13, and 21 depend from independent Claim 6, and dependent claim 31 depends from independent Claim 28. Applicant has shown that each of the independent Claims are allowable. For at least this reason, Applicant respectfully requests reconsideration and allowance of Claims 4, 5, 9, 13, 21, and 31.

Additionally, the Examiner has not made a *prima facie* showing of obviousness with respect to each of these claims. For example, with respect to claims 4, 5, and 31 the Examiner asserts that the combination of *Merkle, Ford*, and *Johnson* is motivated because "it would associate a key to a user with provable certainty." (Final Office Action, page 8) The Examiner does not cite any discussion in *Merkle, Ford*, or *Johnson* to support this contention. Similarly, the Examiner does not cite any portion of *Merkle, Ford*, or *Johnson* to support his motivation contentions with respect to claims 9, 13, and 21. For at least these reasons, Applicant respectfully requests reconsideration and allowance of Claims 4, 5, 9, 13, 21, and 31.

CONCLUSION

Applicant has made an earnest attempt to place this case in condition for immediate allowance. For the foregoing reasons and for other reasons clear and apparent, Applicant respectfully requests reconsideration and allowance of the pending claims.

Applicant believes no fees are due. However, the Commissioner is hereby authorized to charge any fees or credit any overpayments to Deposit Account No. 02-0384 of Baker Botts L.L.P.

If there are matters that can be discussed by telephone to advance prosecution of this application, Applicant invites the Examiner to contact its attorney at the number provided below.

Respectfully submitted,

Baker Botts L.L.P.
Attorneys for Applicant

Bradley S. Bowling
Reg. No. 52,641

Dated: August 4, 2004

CORRESPONDENCE ADDRESS:

Customer No. 05073